Iowa Department of Human Services

Terry E. Branstad **Governor**	**Kim Reynolds** **Lt. Governor**	**Charles M. Palmer** **Director**

Reviewed and Approved

Charles M. Palmer, Director ____________________ Date ____________

Iowa Department of Human Services

Information Security Policy v 1.6

Reviewed May 2011

TABLE OF CONTENTS

Introduction

The purpose of this document is to set guidelines, standards, procedures and policies for the use of and interaction with the Department of Human Service's Enterprise Network, also known as DHS EN.

Authority

Because of both federal and state guidelines on security and administration of data networks and given the fact that it is the responsibility of the Division of Data Management, Department of Human Services (DDM/DHS) to ensure that these guidelines and policies are being met, the following will be implemented. The Division of Data Management is the primary responsible entity for information technology support for the Department of Human Services.

Referenced Documents

All documents, policies, and or guidelines referenced within this document can be found at the Division's Intranet Site, http://dhsintranet/EnterPrisePolicies, within Public Folders on your Outlook client or the DHS Security & Privacy Office Sharepoint site located at http://dhsmoss1/spo/default.aspx.

1. DHS EN Security (User Access, Physical, and Authentication)

Because the Division of Data Management (DDM) is responsible for user management it will be imperative that all requests for access to the DHS Enterprise Network (DHS/EN) use the prescribed security access forms and process as outlined in the "Instructions for Using the Security Information Form". These instructions are located in the Exchange Public Folder accessed via Outlook on your DHS PC. User management will be the sole responsibility of DDM with the full cooperation of the Division to all responsible entities that authorize adding, changing, and deleting of staff as described in the Security Instructions and management directives.

Physical access to state owned computer systems should be monitored at all times by responsible state staff. Computer systems left unmanned, powered on, and in the logged on state are strictly prohibited. All computer systems, if left unattended, at minimum should be logged off and out of the application, the ITS CICS or SNA session, and or DHS Enterprise Network. This means that if a new user sat down at that station before he could use that workstation they would be required to enter their user ID and password. Refer to hard copy "DHS Employee's Manual, I – C, Responsibilities of Department Administrator" or the Department's "DHS Online" book, open "Administration" book, open "General Departmental Procedures" book, open "1–C Confidentiality and Records" section, click on sub section "Responsibilities of Department Administrator" under "CONFIDENTIALITY".

Access to the DHS EN is authenticated by user ID and password, sharing of your ID and password is strictly prohibited. Access to the enterprise network allows the user to access applications (with possible confidential information), internal Intranets, the Internet, gateways (other agencies networks existing behind the ICN firewall) and statewide mail and hub systems. Allowing friends, state staff or vendors to use your logon is the same as sharing confidential information to unauthorized people and is illegal with possible consequences of dismissal.

Access to the DHS/EN by the public or outside state staff (other than DHS staff) will be granted on a per request basis. Responsible DHS staff must authorize along with the appropriate management approval. DHS and the outside entity must establish guidelines as to use of the EN that conforms to this policy and with the appropriate security ensured.

2. DHS Enterprise Network Domain (IADHSR3)

The Division of Data Management, under the direction of the Department of Human Services, will support only a “corporate” view of the Department’s Enterprise Network. This greatly enhances the overall cost, performance, scalability, operability, and support/maintenance of the network.

What this means is the DHS Enterprise Network will be a single (corporate) domain network under the administration and management of the Division of Data Management. User Management, Shares and Permissions, Message Switching, E-Mail, Internet, Intranet, SQL (enterprise data base), Passport (mainframe connectivity), VPN (remote access), and other key components of the enterprise will be centrally administered and managed with the cooperation and coordination of OFS, Child Support, Institutions, Central Office and their extension offices, and other DHS entities.

Rogue servers (servers set up without the cooperation and coordination of DDM) and independent or separate domains (local area networks or wide area networks separate from IADHSR3 domain) will not be allowed or accepted.

3. DHS EN NT Administrator Authentication, (Domain Admin Rights)

Only staff assigned to the Department’s Enterprise Wide Area Network team within the Division of Data Management will have enterprise network administrator rights.

This means that any state staff or DHS contracted staff that has Domain Administrator rights will report directly to the Division of Data Management. That before any DHS, other Department’s or Contract staff are given EN Windows Server administrative rights they must be assigned to the Bureau of Network Support, Division of Data Management, Department of Human Services or under a contract that is monitored and supervised by the Division of Data Management.

The strict adherence to the policies for “Domain administrator rights” as described above is required to ensure that both Federal and State guidelines and mandates are being met and for the proper and adequate management of the Department’s Enterprise Network. It is imperative that this policy be adhered to; this will ensure the reliability, security, performance and operability of the entire Department’s Enterprise Network as required by the 5,200 plus users using this network system within the Department of Human Services.

4. Windows Server Enterprise Network Trust Relationships

That all trusts (bridges between other NT domains or LAN Networks) built between the DHS EN (IADHSR3) and any other domain or network (state or private) be one way only and under the management of DDM/DHS.

Example; Outside domains or networks can trust us but we will NOT trust that network or domain unless authority is granted by DHS senior management and all security requirements are met according to all state and federal policies and guidelines.

5. DAS Directory Service

With the deployment of a central “directory” under the management of the department of Administrative Services (DAS/ITE) and direction given by that department and the Governor’s Office the use of independent site connectors will no longer be required or permitted.

The DAS Global Directory provides directory services between the state agencies’ diversified mail systems.

6. DHS Enterprise Network Infrastructure, Statewide (WAN), Local Office (LAN), and Institution or Campus (CAN)

That the design, specifications, requirements, selection of network components and implementation of the Department’s infrastructure will be the responsibility of the Division of Data Management, Department of Human Services working with ICN and DAS-ITE.

This is required to ensure a statewide corporate view of a secured data network that takes all aspects of data, applications and messaging into consideration, not only between all entities of DHS but other agencies, states and federal systems as well.

This includes the network servers, hubs, switches, internal routers, ups systems and wiring at any DHS local site or institution. Internal data fiber, termination of data fiber or risers also falls under the responsibility of DDM. Edge routers (routers that connect to the ICN) and LEC (local exchange carriers)
will be coordinated by DDM/DHS and ICN. All of this equipment will be administered and managed by the DDM/DHS and ICN using Network management tools (i.e., HP Openview) with the cooperation of local and institution IT staff.

7. Customer Service Support Center (Help Desk)

The Division of Data Management will provide a central support center or help desk with a single telephone number to respond to all DHS EN problems, concerns and questions. This support center will be available and staffed from 7 AM until 5 PM Monday through Friday with the exception of holidays.

Off hours will be supported by calling the Help Desk phone number which will roll over to the Emergency On-Call phone. After hours support is defined as emergency support for systems such as E-mail down. Emergency support is available from DDM seven days a week twenty-four hours a day.

Calling for help / assistance, on hours / off hours, and EN Support structure

The Division's Enterprise Network "Help Desk" is known as the Technical and Network Support Center (TNSC).

TNSC telephone numbers are:

- *Local calls Des Moines area (515) 281-4694*
- *Toll calls should use (800) 922-8905*

TNSC normal hours are Monday through Friday, 7:00am until 5:00pm, excluding holidays.

TNSC off hours are 5:00pm until 7:00am Monday through Friday and all day Saturday, Sunday and official state holidays.

Emergency calls for Enterprise Network are handled by TNSC, during working hours TNSC will contact the appropriate LAN administrator (ICN, DHS, or ITE) to assist with resolution. *Before or after normal hours, holidays or on weekends TNSC voice mail message will ask the caller to hold the line if they have an emergency ((i.e., server down, router down, Exchange down (mail services) or in general no network connectivity)). Call will roll over to On Call Support Person.*

EN WAN/LAN off hour on call support staff (515-681-4944) will try to resolve the problem or contact the proper staff person who will return the call within 30 minutes and take appropriate action.

8. Windows Shares and Permissions (Secured, private and public)

Because the Division of Data Management is responsible for user directory services it will be imperative that all requests for access to shares and/or disk space on the DHS Enterprise Network (DHS/EN) use the prescribed security access forms and process as outlined in the "Security Forms Instructions". Disk allocation, directory shares and permissions will be the sole responsibility of the Division of Data Management with full cooperation of the Division to all responsible entities that authorize adding, changing, and deleting of staff access to shares and disk files as describe in the Security Instructions and management directives.

9. Supported Software on EN (Network, User Productivity, and Application)

The Division of Data Management will set software standards and ensure conformity of based on understanding the agencies' business needs.

It is important that all DHS staff purchasing, installing or planning to implement any software on any PC, client workstation, or server that is integral parts of the DHS EN refer to "Current Software Standards" on Page 6 of this document. Contained in this document is further information on operating systems, productivity tools, and application software compatibility and implementation goals. Staff must also review any software purchases and or implementation of same with the EN WAN/LAN staff for the proper planning and implementation procedures.

The current software standards are as follows:

Network Software

- Windows Server 2003
- MS SCCM
- MS Exchange 2003
- Cisco Secure 2.4
- MS SQL 2000, 2005 and 2008
- Norton Corporate Edition

User Productivity/Client Software Installed on User's PC's

- Windows XP SP 2 & 3
- MS Office 2007 (Earlier versions are supported with the understanding that the direction is for all users to move to the prescribed standard).
- Passport
- MS Outlook 2007
- Norton Antivirus Corporate Edition
- MS Internet Explorer (IE Browser) 7.0 Service Pack 1
- Adobe Acrobat Reader 6.0.1

To ensure the reliability of desktop performance and the operation of the enterprise it will be imperative that NO software be downloaded from the Internet, purchased privately, or acquired by any other means and implemented anywhere on the Enterprise Network without the prior approval of the Division of Data Management.

Software (desired/required) not listed above must be cleared through management and then tested by the Division for compatibility, proper licensing, virus-free and workability (proper coding and structure) with the agencies enterprise network and applications before implementing.

10. Supported Hardware on EN (Server, Client (PC), Network Component

The Division of Data Management will set hardware standards and ensure conformity of based on understanding the agencies' business needs.

The current hardware standards are as follows:

Servers
Current supported vendors:
· Dell – Various Models

PC, Workstation and Laptops
Current supported vendors:
· HP – Various Models

Minimum Requirements, Desktops and Laptops, when purchasing new systems
· Core 2 duo CPU running at 2.4 GHz
· 80 GB Hard Drive
· Multimedia Equipped
· 100/1000 Ethernet Adapter
· 2.9 GB RAM
· 128kb V90 Modem (notebooks only)

Network Components
. Cat 5 Wiring
. Cisco Hubs
. Cisco Access Servers
. Cisco Switches
. Cisco Core Switches with VoIP capability
. Cisco Routers
. Nortel Edge Routers (managed by ICN)
· PIX 501
· Dell Switches

The Division of Data Management will allow only state owned equipment to be a part of, connected to, or used on the DHS Enterprise Network. This includes all computer workstations, printers, network communication devices (hubs / switches / routers) and servers.

No personal computers, laptops or otherwise will be allowed to connect to the enterprise network either through an Ethernet connection or a dial up connection.

Any equipment (PC's, Servers, Printers, Switches or Routers) or software attached to or any part of the DHS Enterprise Network will be placed under the management and administration of the Division of Data Management (ENAM Team) during the duration of this attachment. This does include all hardware and software owned or purchased by entities other than DHS.

11. Purchasing of EN Software or Hardware

That all software and hardware that will interact with or be an integral part of the DHS/EN must go through the DDM purchase process which is describe as follows:

- Planning session involving DDM EN WAN/LAN Administrators.
- This must include compatibility issues, capacity, ongoing maintenance, administration and support.
- Funds approved by appropriate management staff including ongoing and support costs.
- Completion of purchase approval form "Iowa Department of Human Services Approval for Purchase".
- Appropriate signatures affixed.
- All replaced hardware (servers, PC's, hubs, switches, etc.) is the property of DHS and will be managed by the Division of Data Management.

Requests to use or put in service replaced equipment must be cleared through the Division of Data Management.

The copying of software from one system to another is not allowed without compatibility and capacity review by DDM EN staff and in most cases illegal. Do not do without first consulting with DDM.

12. DHS EN NT Internet / Intranet

Please refer to "DHS SQL Policies" created by DHS on the Division's Intranet site.

Please refer to “DHS Internet Project Development Policies and Standards ” created by DHS on the Division’s Intranet site.

Please refer to “DHS Intranet Project Development Policies and Standards ” created by DHS on the Division’s Intranet site.

Please refer to “ DHS Internet Usage Policy & Procedures” also residing on the Division’s Intranet Site.

The DHS Intranet Web Site’s URL or address is http://dhsintranet

Implementation, administration and support of the Agencies Internet/Intranet Servers will be the responsibility of the Division of Data Management.

All DHS production Intranet and Internet sites and or pages will physically reside on the provided servers and data bases of DDM and fall under the before mentioned guidelines and procedures under the guidance of the assigned DDM Web Master.

13. DHS EN Remote Access Services

All users of the DHS EN which desire to access the network remotely will be required to submit a remote access form to DDM requesting VPN authentication signed by the appropriate management. User access will be governed by the users current EN access rights.

Remote access to the enterprise network will be through the Division’s Remote Access Server, CISCO AS5300 with Cisco Secure remote authentication. Under NO circumstances will it be permitted to set up remote access services (RAS) on any DHS EN Server, Workstation, or Windows Workstation.

14. Exchange (Mail / Email) Services

Please refer to “DHS Email Use & Encryption Policy and Procedures”.

15. Personal use and/or inappropriate use of the DHS EN

Using the state’s Internet Infrastructure or the Department’s Enterprise Network for personal use from your home PC is prohibited, i.e. Internet or electronic mail from POP3 servers or ISP’s.

Using the network for inappropriate exchange of data is prohibited, i.e., jokes, pornography, confidential information, or personal issues.

There will be no use or attachment of personally owned equipment (PC's, printers, or network data communication devices) on the Department's Enterprise Network.

16. DHS Enterprise Network Backup & Restore / Disaster Recovery Solutions & Policies

Refer to the DHS's **"DHS Backup and Restore Policy".**

Refer to the DHS's "Contingency Planning Policy".

17. Application Development

The Division of Data Management must establish all application development that needs to be a part of, run on, or go through the DHS Enterprise Network. This means all development be initiated (rather developed by or not) and followed through on by the Division's application Bureaus.

All application development, rather developed internally by DDM application staff for customers, developed by vendors under contract with the Division, or developed by an entity within the agency working with a particular application bureau, must from conceptual design through implementation, be planned, designed, tested and installed with close working relationship of the enterprise network teams if it is to be made an integral part of the department's enterprise network.

Resources required to add, maintain and support (people, hardware and software) from the Enterprise perspective must be provided and budgeted by the requestor.

Client/Server application development using Web or SQL Data Base technologies needs to follow standards and procedures developed by the Division of Data Management and located on the Division's Intranet page.

Refer to the DHS's "DHS SQL Standards".
Refer to the DHS's "DHS Internet Project Development Policies & Standards".
Refer to the DHS's "DHS Intranet Project Development Policies & Standards".
Refer to the DHS's "DHS Internet Usage Policy".
Refer to the DHS's "Web Authority Guidelines".

Questions, modification and or enhancements to this document "Enterprise Network Security, Administration and Management Policies" please contact the Division of Data Management, Bureau of Network Support, attention Cathy McLuen (515) 281-5775 or email cmcluen@dhs.state.ia.us. You may also contact the EN Help Desk who will forward requests to the appropriate staff.

Cathy McLuen, Chief
Bureau of Network Support
Division of Data Management
Department of Human Services